Assessing Cybersecurity Knowledge, Attitudes, and Practices (KAP) Among First-Year Information Technology Students at HGBaquiran College

A Research Presented
to the Undergratuate School
HGBaquiran College, Inc.
Tumauini, Isabela

In Partial Fulfillment
of the Requirements for the Degree
BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

Researchers:

Aquino, Clarisa U.
Bacani, Kristel Ann M.
Baccay, Jay Christian
Cayaba, Instien L.
Diaz, Jesus D.

November 2025

APPROVAL SHEET

In partial fulfillment of the requirements for the degree, BACHELOR OF SECONDARY EDUCATION MAJOR IN ENGLISH, this study titled, _____, has been prepared and submitted by JUAN B. CRUZ, who is hereby recommended for Oral Examination.

_____
Adviser

_____
Data Consultant

_____
Language Editor

Approved by the Panel for Oral Examination with a grade of PASSED.

PANEL OF EXAMINERS

PEDRO B. PENDUKO, PhD
Chairperson

PEDRO PENDUKO, PhD
Member

PEDRO B. PENDUKO, DME
Member

PEDRO B. PENDUKO, DPA
Member

PEDRO B. PENDUK, DME
Member

Accepted and approved in partial fulfillment of the requirements for the degree, BACHELOR OF SECONDARY EDUCATION MAJOR IN ENGLISH.

PEDRO B. PENDUKO, PhD
Program Coordinator, BSEd

ROYETE B. GUILLERMO, LPT
Research Coordinator

ACKNOWLEDGMENT

We sincerely extend our deepest gratitude to everyone who played a part in the success of this research.

To **Mr. Raffy A. Melegrito,** our adviser, we express our heartfelt thanks for your invaluable guidance, insightful suggestions, and unwavering support throughout the course of this study. Your expertise and dedication greatly contributed to the development and completion of this project.

To **HGBaquiran College** and the **Information Technology Department,** we thank you for providing the resources, platform, and encouragement that allowed us to turn our ideas into reality.

To our **families** and **friends,** we are deeply grateful for your love, understanding, and continous support, especially during times of uncertainty and difficulty. Your encouragement inspired us to stay focused and motivated in achieving our goals.

To our **respondents,** including the **faculty members**, we truly appreciate your time, cooperation, and valuable insights, which were vital to the success of this research.

Above all, we give thanks to **God Almighty** for granting us the strength, determination, and wisdom to accomplish this study.

~ The Researcher's

DEDICATION

This research is wholeheartedly dedicated to our beloved parents, who have been our constant source of strength and inspiration. In times when we doubted ourselves, you never failed to provide moral, emotional, spiritual, and financial support. Your love and sacrifices motivated us to keep going and make this endeavor possible.

To our relatives, instructors, friends, brothers, sisters, and classmates – thank you for your words of encouragement, guidance, and motivation that helped us perserve until the completion of this study.

Lastly, we dedicated this work to Almighty God, for His unending guidance, wisdom, and strength, and for blessing us with good health and determination throughout this journey.
All honor and glory belong to You.

ABSTRACT

As digital natives entering higher education, first-year Information Technology (IT) students are often perceived as tech-savvy, yet their actual vulnerability to cyber threats is a critical concern. This quantitative, descriptive-correlational study sought to assess the level of cybersecurity awareness among 100 first-year IT students at HGBaquiran College. The study utilized a researcher-made survey questionnaire structured around the Knowledge, Attitude, and Practice (KAP) framework.

Data analysis revealed a 'Moderate' level of knowledge (M=5.48/10), with critical deficiencies in recognizing dynamic threats like phishing and social engineering. Students demonstrated a 'Positive' attitude towards cybersecurity (M=3.69) but displayed a concerning level of overconfidence that was not supported by their knowledge scores. Cybersecurity habits were performed 'Often' (M=3.88), but practices requiring specific technical knowledge lagged, confirming a significant KAP gap.

The primary finding from the inferential analysis was a statistically significant, weak positive correlation between Age and Attitude ($r = .211$, $p = .035$), suggesting that maturity influences mindset but not skill. No other demographic variables (gender, internet use) were significant predictors of knowledge, attitude, or practice. The study concludes that despite good intentions, students lack the specific knowledge required to translate positive attitudes into effective security practices. Therefore, the study strongly recommends the implementation of a mandatory, hands-on cybersecurity training module in the first-year curriculum to bridge the identified KAP gap and cultivate a more resilient security culture.

TABLE OF CONTENTS

Content **Page**

TITLE PAGE i

APPROVAL SHEET ii

ACKNOWLEDGEMENT iii

DEDICATION iv

ABSTRACT v

TABLE OF CONTENTS vi

LIST OF TABLES vii

LIST OF FIGURES viii

Chapter I. INTRODUCTION

Background of the Study 1

Statement of the Problem 2

Significance of the Study 3

Scope and Delimitation 4

Chapter II. REVIEW OF RELATED LITERATURE

Related Literature 5

Foreign Studies 6

Local Studies 7

Synthesis 7

Theoretical Framework 8

Conceptual Framework 9

Hypothesis of the Study 10

Definition of Terms 11

Chapter III. METHODOLOGY

Research Design 12

Respondents of the Study 12

Sample and Sampling Procedure 13

Data Gathering Instruments 14

Data Gathering Procedures 15

Statistical Tool 15

Chapter IV. RESULTS, ANALYSIS, AND

Interpretation of Data 17

Chapter V. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

Summary 24

Conclusion 25

Recommendation 26

BIBLIOGRAPHY 28

APPENDICES 30

Appendix A: Letter 31

Appendix B: Survey Questionaire 32

Appendix C: Raw Scores 35

Appendix D: Certifications 38

CURRICULUM VITAE 40

LIST OF TABLES

Table No.	Title	Page No.
Table 1	Frequency and Percentage Distribution of Respondents by Age	17
Table 2	Frequency and Percentage Distribution of Respondents by Gender	18
Table 3	Frequency and Percentage Distribution by Daily Internet Use	18
Table 4	Summary of Correct Responses for Knowledge Assessment (N=100)	19
Table 5	Weighted Mean of Attitude Towards Cybersecurity	20
Table 6	Weighted Mean of Cybersecurity Practices	21
Table 7	Correlation Between Demographic Profile and Cybersecurity Awareness	22

LIST OF FIGURES

Table No.	Title	Page No.
Figure 1	Coceptional Framework of the Study	10

Chapter I

THE PROBLEM AND ITS BACKGROUND

Background of the Study

In an era defined by ubiquitous connectivity and digital transformation, cybersecurity has evolved from a niche technical concern into a fundamental aspect of daily life. Individuals, corporations, and educational institutions are increasingly reliant on digital infrastructure, making them prime targets for a wide array of cyber threats, including phishing, malware, ransomware, and identity theft. The global landscape is witnessing a surge in sophisticated cyberattacks, creating an urgent need for a proactive and security-conscious populace, a challenge that is particularly acute within higher education institutions (Al-Ghafis et al., 2022).

University students represent a particularly vulnerable demographic. As "digital natives," they engage heavily in online activities, utilize multiple devices, and frequently connect to public networks. However, research consistently shows that their technical fluency does not automatically translate into sound cybersecurity awareness. This gap between high technology usage and low security consciousness makes them susceptible to attacks that can lead to data loss, financial fraud, and compromised academic integrity (Portela & Tovar, 2023).

This issue is critically amplified for students pursuing a degree in Information Technology (IT). These students are not merely users of technology; they are its future architects, developers, and protectors. Studies show that even among IT and engineering students, there can be significant deficiencies in security knowledge and practices (Al-Mhiqani et al., 2022). A lack of awareness in this cohort is a significant concern, as it indicates a potential weakness in the future workforce responsible for safeguarding digital assets.

At HGBaquiran College, first-year IT students are at the nascent stage of their professional formation. They are building the fundamental knowledge that will underpin their entire career. However, the level of their pre-existing cybersecurity awareness which is spanning their knowledge of threats, attitudes towards security protocols, and actual online behaviors—is currently unknown. Establishing a clear baseline of their awareness is the first and most critical step in identifying knowledge gaps and developing targeted educational interventions. Therefore, this research seeks to conduct a comprehensive assessment of the cybersecurity awareness among first-year IT students to provide data-driven insights for strengthening the curriculum and fostering a culture of security from the very beginning of their academic journey.

Statement of the Problem

This study aims to assess the level of cybersecurity awareness among first-year Information Technology students at HGBaquiran College during the Academic Year 2025-2026. The results of this study will serve as a basis for a proposed cybersecurity enhancement program.

Specifically, it seeks to answer the following questions:

1. What is the demographic profile of the respondents in terms of:
    1.1. Age;
    1.2. Gender; and
    1.3. Frequency of internet use.
2. What is the level of cybersecurity awareness of the respondents as measured by their:
    2.1. Knowledge of cybersecurity concepts and threats;
    2.2. Attitudes towards cybersecurity best practices; and
    2.3. Practices in their personal online activities.

3. Is there a significant relationship between the demographic profile of the respondents and their level of cybersecurity awareness (Knowledge, Attitudes, and Practices).
4. Based on the findings of the study, what targeted action plan can be proposed to enhance the cybersecurity awareness of first-year IT students.

Significance of the Study

The findings of this research will provide significant benefits to various stakeholders:

- **Students.** This study will provide them with a clear understanding of their own strengths and weaknesses in cybersecurity awareness. The results will highlight areas where they need to be more cautious, directly contributing to their personal online safety and professional development.
- **IT Department Faculty.** The research will offer empirical data on the baseline knowledge of incoming students. This will enable instructors to tailor their teaching methods, identify gaps in the early-stage curriculum, and emphasize specific security topics that are found to be lacking.
- **HGBaquiran College Administration.** The findings will inform the administration about the risk profile of its student body and can be used to develop and justify campus-wide cybersecurity policies, awareness campaigns, and training programs, thereby enhancing the overall security posture of the institution.
- **Future Researchers.** This study will serve as a foundational piece of literature for the HGBaquiran College community. Future researchers can use these findings as a baseline to conduct longitudinal studies, track improvements over time, or expand the research to other departments or year levels.

Scope and Delimitation

This study will focus on assessing the Knowledge, Attitudes, and Practices (KAP) related to cybersecurity awareness. The research is confined to all officially enrolled first-year Information Technology (IT) students at HGBaquiran College for the Academic Year 2025-2026. Due to the manageable size of the population, a census method will be employed, inviting all members of the population to participate.

The primary data-gathering instrument will be a researcher-made survey questionnaire designed to measure the variables specified in the statement of the problem.

This study will not cover students from other departments or year levels within the college. It will neither measure the technical proficiency of students in implementing security tools *(e.g., configuring firewalls or conducting penetration tests)* nor will it assess the effectiveness of the college's existing network infrastructure security. The study is limited to the students' self-reported awareness and behaviors, not their observed technical skills.

Chapter II

REVIEW OF RELATED LITERATURE

This chapter presents a review of relevant literature and studies that are significant to the focus of this research. It is organized into several key sections: a review of foreign and local studies concerning cybersecurity awareness among students, a synthesis of the literature that identifies the research gap, the theoretical and conceptual frameworks that guide the study, the research hypothesis, and the operational definition of key terms.

Related Literature

The literature on cybersecurity awareness establishes it as a critical, non-technical countermeasure to the growing prevalence of cyber threats. It is widely acknowledged that technology alone, such as firewalls and antivirus software, is insufficient to protect systems. The human element is often cited as the weakest link in the security chain, making user education and awareness paramount (Hadlington, 2017). Awareness is typically deconstructed into three key measurable dimensions: knowledge of risks and protective measures, attitudes and perceptions towards security behaviors, and the actual implementation of these behaviors in practice. This tripartite model, often referred to as Knowledge, Attitude, and Practice (KAP), provides a comprehensive framework for assessing an individual's overall security posture.

Foreign Studies

International research consistently highlights vulnerabilities among university students. A study by Portela and Tovar (2023) in Portugal investigated the cyber risk perception and training needs of undergraduates. They found that while students are confident in their digital skills, they simultaneously exhibit risky online behaviors and a low perception of personal threat, reinforcing the "digital

native paradox." The study concluded that higher education institutions have a crucial role to play in formalizing cybersecurity training to bridge this gap. This is directly relevant as it underscores the need to assess, rather than assume, the awareness level of tech-savvy students.

Specifically focusing on technical students, a study by Al-Mhiqani et al. (2022) in Yemen assessed the cybersecurity awareness among IT and engineering students. Their findings were revealing: despite their technical field of study, a significant portion of students showed deficiencies in critical areas like password management, phishing identification, and understanding of malware. The study stressed that a specialized academic background in IT does not guarantee high cybersecurity awareness, making a focused assessment within this cohort essential. This affirms the rationale for focusing squarely on the IT students at HGBaquiran College.

In a similar vein, Al-shboul et al. (2023) utilized the KAP model to survey university students in Jordan. Their results indicated that while students generally had moderate knowledge and positive attitudes towards cybersecurity, their practices were often poor. For instance, students agreed that strong, unique passwords were important (Attitude) but admitted to reusing passwords across multiple sites (Practice). This common disconnect between attitude and practice is a central theme in cybersecurity literature and a key area of investigation for the current study.

Furthermore, research by Yaokumah et al. (2020) in the UAE examined the factors influencing students' intentions to comply with information security policies. They found that students' "perceived vulnerability" to threats and their "self-efficacy" (confidence in their ability to perform security behaviors) were strong predictors of their intention to act securely. This suggests that awareness campaigns should not only provide knowledge but also aim to increase students' confidence and their understanding of personal risk.

Local Studies

In the Philippines, cybersecurity awareness has become a prominent national concern, especially with the implementation of the Data Privacy Act of 2012 *(RA 10173)*. Research within the country reflects the global trends. A study conducted by Tanael et al. (2021) among Filipino university students revealed that while most were aware of basic threats like viruses and hacking, their knowledge of more nuanced social engineering attacks like phishing was significantly lower. The study recommended the integration of practical and context-specific cybersecurity education into the curriculum.

Olegario (2022) examined the awareness and practices of senior high school students in the Philippines, a population on the verge of entering university. The study found a similar pattern of moderate awareness but inconsistent protective behaviors, particularly regarding sharing personal information online and using public Wi-Fi securely. This indicates that students may be entering higher education, including IT programs, with pre-existing vulnerabilities, reinforcing the need for baseline assessment at the first-year level.

Moreover, Pitagan (2021), in a discussion of digital citizenship in the Philippine context, argued that education must move beyond technical skills to include critical thinking and ethical behavior online. This holistic view frames cybersecurity awareness not just as self-protection but as a civic responsibility. The current research aligns with this perspective by assessing attitudes and practices, which are components of responsible digital citizenship.

Synthesis

The reviewed literature, from both foreign and local sources, collectively establishes a clear consensus: cybersecurity awareness is a critical yet often deficient area among university students. A recurring theme is the paradox of the "digital native," where high

technological proficiency coexists with risky online behavior. Furthermore, studies consistently demonstrate a significant gap between students' knowledge/attitudes and their actual practices (Al-shboul et al., 2023; Tanael et al., 2021).

While these studies confirm the problem on a broad scale, a specific gap exists in the literature. There is a need for highly contextualized, institution-specific research that uses a structured framework like KAP to provide actionable data for curriculum development. This study addresses this gap by focusing specifically on the first-year Information Technology cohort at HGBaquiran College. By conducting a census of this crucial group, the research will provide a precise, data-driven baseline that is not generalized from other populations, but is directly applicable to the faculty, administration, and students of the IT department.

Theoretical Framework

This study is anchored on the Unified Theory of Acceptance and Use of Technology (UTAUT), proposed by Venkatesh, Morris, Davis, and Davis (2003). The UTAUT model is a leading theoretical framework in Information Systems research, designed to explain user intentions to use a technology and their subsequent usage behavior. It synthesizes constructs from eight prominent preceding models, providing a comprehensive view of the determinants of technology acceptance.

In the context of this study, "technology" is broadly defined to include specific security tools *(e.g., antivirus software, password managers)*, features *(e.g., two-factor authentication)*, and security-conscious practices. The UTAUT model posits that four key constructs directly influence a user's behavioral intention and use behavior:

1. **Performance Expectancy:** This is the degree to which an individual believes that using the system (or practice) will help

them attain gains in job performance or, in this context, personal security.

- *Application:* An IT student's belief that using strong, unique passwords will significantly improve the protection of their online accounts.

2. **Effort Expectancy:** This is the degree of ease associated with the use of the system.
    - *Application:* How easy or difficult a student perceives the process of setting up and using two-factor authentication on their accounts.
3. **Social Influence:** This is the degree to which an individual perceives that important other (e.g., peers, instructors, family) believe they should use the new system.
    - *Application:* The influence of IT professors and classmates recommending the use of specific security practices, shaping a student's intention to adopt them.
4. **Facilitating Conditions:** This is the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system.
    - *Application:* The availability of resources like college-provided software, clear instructions, or helpdesk support that make it easier for students to implement secure practices.

According to the UTAUT model, these four constructs are direct determinants of Behavioral Intention, which in turn influences Use Behavior. The model provides an ideal framework for this research because it moves beyond general awareness to explore the specific perceptual drivers—utility, ease of use, social pressure, and support systems—that will likely determine whether HGBaquiran College's first-year IT students translate their cybersecurity knowledge into consistent, protective action

Conceptual Framework

The research follows an Input-Process-Output (IPO) model to illustrate the relationship between the study's variables.

INPUT: This box contains the primary variables that serve as the basis for the investigation. This includes the Demographic Profile of the first-year IT students *(age, gender, frequency of internet use)* and the core concepts of Cybersecurity Awareness (Knowledge, Attitudes, and Practices) that will be measured.

PROCESS: This involves the methods used to collect and analyze the data. It includes the administration of a survey questionnaire to the respondents via a census approach and the subsequent statistical analysis of the gathered data, including descriptive statistics and correlational analysis.

OUTPUT: This is the expected outcome of the study. Based on the analysis of the findings, the primary output will be a **Proposed Cybersecurity Enhancement Program** tailored to address the identified weaknesses in the Knowledge, Attitudes, or Practices of the first-year IT students.

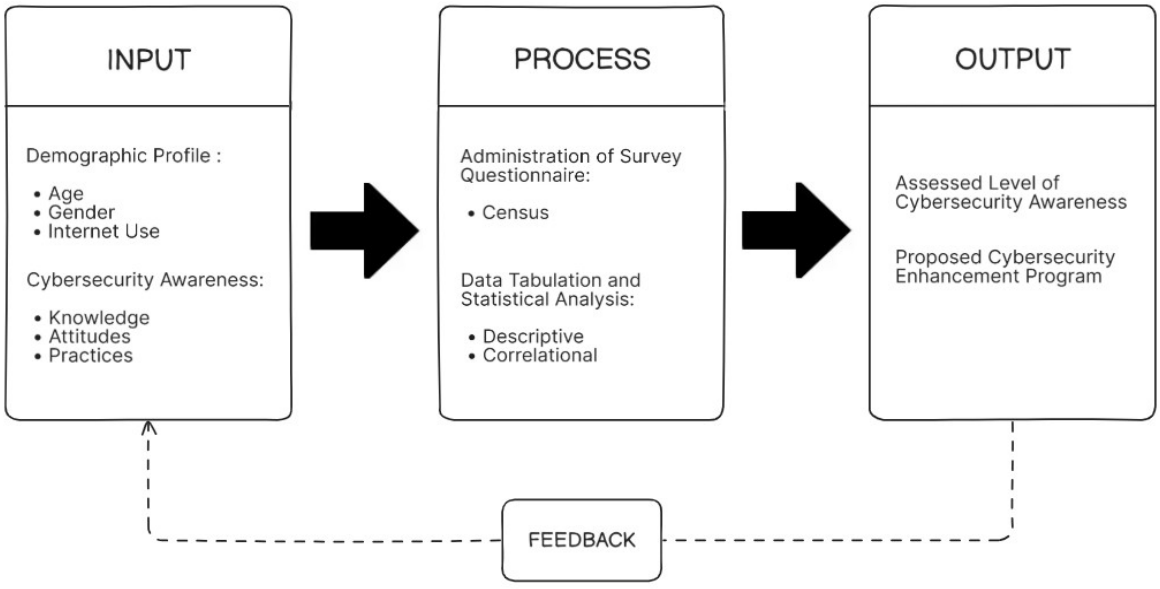

Figure 1. Conceptual Framework of the Study

Hypothesis of the Study

In line with the third specific research question, the study will test the following null hypothesis (H_0) at a 0.05 level of significance:

H_0: There is no significant relationship between the respondents' demographic profile *(age, gender, frequency of internet use)* and their level of cybersecurity awareness in terms of Knowledge, Attitudes, and Practices.

Definition of Terms

For clarity and consistency, the following key terms are operationally defined as they are used in this study:

- **Cybersecurity Awareness.** The composite level of understanding and consciousness possessed by a student, measured through the combined scores of their cybersecurity knowledge, attitudes, and practices.
- **Knowledge.** This refers to the respondents' objective understanding of fundamental cybersecurity concepts, common threats *(e.g., phishing, malware)*, and best practices, as measured by multiple-choice questions in the survey.
- **Attitudes.** This refers to the respondents' expressed feelings, beliefs, and perceptions regarding the importance of cybersecurity measures, as measured by a Likert scale in the survey.
- **Practices.** This refers to the respondents' self-reported frequency of performing specific security-related behaviors and actions in their personal online activities, as measured by frequency scales in the survey.
- **First-Year IT Students.** This refers to all individuals officially enrolled in the first-year level of the Bachelor of Science in Information Technology program at HGBaquiran College during the Academic Year 2025-2026.
- **KAP Model.** A framework used in this study to structure the assessment of cybersecurity awareness by breaking it down into three distinct components: Knowledge, Attitudes, and Practices.

Chapter III

METHODOLOGY

This chapter presents the methodology that will be employed in the study. It includes a detailed description of the research design, the respondents, the sampling procedure, the data gathering instrument, the data gathering procedure, and the statistical tools that will be used for data analysis.

Research Design

The study will utilize a quantitative, descriptive-correlational research design. It is quantitative because it involves the collection of numerical data through a survey questionnaire and the use of statistical analysis to interpret the findings.

The design is descriptive as it aims to systematically describe the demographic profile of the first-year IT students and their level of cybersecurity awareness in terms of Knowledge, Attitudes, and Practices (KAP). This component addresses the "what is" aspect of the research, corresponding to the first and second research questions.

The design is also correlational because it seeks to determine the nature and significance of the relationship between the students' demographic profiles and their respective levels of cybersecurity awareness. This component addresses the third research question, investigating if variables change in relation to one another.

Respondents of the Study

The respondents of this study will be all the officially enrolled first-year Bachelor of Science in Information Technology (BSIT) students at HGBaquiran College for the Academic Year 2025-2026. The total population for this cohort is N = 100.

Sample and Sampling Procedure

The total population of first-year IT students is N = 100. To determine a statistically robust sample size for this population with a 5% (0.05) margin of error, Slovin's formula would typically be applied:

Formula:

$$n=\frac{N}{1+Ne^2}$$

Where:

$n = sample ¿¿$

$N = total population$

$e = margin of error$

Calculation:

1. n = 100 / (1 + 100 * (0.05)^2)
2. n = 100 / (1 + 100 * 0.0025)
3. n = 100 / (1 + 0.25)
4. n = 100 / 1.25
5. n = 80

The calculation indicates a required sample size of 80 students. However, since the required sample (n=80) constitutes a very large proportion (80%) of the total population (N=100), the researcher has decided to use a census method instead of sampling. A census involves inviting every single member of the population to participate. This approach is more advantageous for a population of this size as it eliminates sampling error, maximizes statistical power, and ensures that the findings are a complete and accurate representation of the entire target group.

Therefore, all 100 first-year IT students were invited to be the respondents of this study.

Data Gathering Instruments

The primary instrument for this study will be a researcher-made survey questionnaire. The questionnaire will be structured to directly answer the statement of the problem and will be divided into four parts:

- **Part I: Demographic Profile.** This section will gather the respondents' demographic information, including age, gender, and frequency of internet use.
- **Part II: Knowledge of Cybersecurity.** This section will assess the respondents' factual knowledge of cybersecurity concepts, threats, and preventative measures. It will consist of multiple-choice questions with one correct answer and several distractors.
- **Part III: Attitudes Towards Cybersecurity.** This section will measure the respondents' perceptions, beliefs, and feelings about the importance of cybersecurity practices. It will use a 5-point Likert scale as follows:

Point	Verbal Interpretation
5	Strongly Agree
4	Agree
3	Neutral
2	Disagree
1	Strongly Disagree

- **Part IV: Cybersecurity Practices.** This section will assess the respondents' self-reported frequency of performing secure online behaviors. It will use a 5-point frequency scale as follows:

Point	Verbal Interpretation
5	5 - Always
4	4 - Often

3	3 - Sometimes
2	2 - Rarely
1	1 - Never

Prior to its administration, the questionnaire will undergo content validation by a panel of three (3) experts in the fields of Information Technology and Research to ensure its clarity, relevance, and accuracy. A pilot test with a small group of second-year IT students will also be conducted to check for any ambiguity in the questions.

Data Gathering Procedure

The researcher will follow a systematic procedure to ensure the ethical and efficient collection of data:

1. **Request for Approval.** The researcher will submit a formal letter to the Dean of the College of Information Technology, seeking permission to conduct the study and to obtain the official list of first-year IT students.
2. **Preparation of Instruments.** Upon approval, the researcher will prepare the final survey questionnaires, either in printed form or via a digital platform like Google Forms.
3. **Administration of the Questionnaire.** The researcher will coordinate with the relevant instructors to find a suitable time to administer the survey. Before distributing the questionnaire, the researcher will explain the study's purpose, assure the respondents of the confidentiality of their responses, and confirm their voluntary participation.
4. **Collection and Retrieval.** The researcher will collect the accomplished questionnaires immediately after the respondents have finished. For online surveys, responses will be downloaded from the platform.

5. **Data Processing.** The collected data will be tabulated, encoded, and prepared for statistical analysis using appropriate software.

Statistical Treatment of Data

The data gathered will be analyzed using the following statistical tools to answer the specific research questions:

1. **Demographic Profile:**
    - **Frequency and Percentage Distribution.** This will be used to summarize the demographic profile of the respondents in terms of age, gender, and frequency of internet use.
2. **Level of Cybersecurity Awareness - KAP:**
    - **Weighted Mean.** This will be used to determine the central tendency of responses for the Attitude and Practice sections of the questionnaire. The following scale will be used for interpretation:

Range	Verbal Interpretation
4.21 - 5.00	Very High
3.41 - 4.20	High
2.61 - 3.40	Moderate
1.81 - 2.60	Low
1.00 - 1.80	Very Low

3. **Relationship between Variables:**
    - **Pearson Product-Moment Correlation (Pearson's r).** This will be used to measure the strength and direction of the linear relationship between the respondents' demographic profile variables (when treated as ordinal or scale data) and their scores on the Knowledge, Attitude, and Practice sections.

4. **Proposed Action Plan:**
    - The proposed action plan will be formulated based on the descriptive analysis of the findings, particularly focusing on the indicators in the Knowledge, Attitude, and Practice sections that receive the lowest scores or mean ratings.

Chapter IV

RESULTS, ANALYSIS, AND INTERPRETATION OF THE DATA

This chapter presents the data gathered from the 100 first-year IT students at HGBaquiran College. The results are organized according to the research questions posed in this study. Each section provides a presentation of the data, a statistical analysis, and a detailed interpretation of the findings related to the respondents' demographic profile, their level of cybersecurity awareness, and the relationship between these variables.

1. Demographic Profile of the Respondents

The first research question sought to determine the demographic profile of the respondents in terms of age, gender, and daily internet use.

Age. The age distribution of the respondents is presented in Table 1.

Table 1: Frequency and Percentage Distribution of Respondents by Age

Age	Frequency (f)	Percentage (%)
17	13	13.0%
18	50	50.0%
19	17	17.0%
20	3	3.0%

Age	Frequency (f)	Percentage (%)
21	4	4.0%
24	3	3.0%
27	2	2.0%
35	1	1.0%
Total	**100**	**100.0%**

As shown in Table 1, half of the respondents (**50.0%**) are 18 years old. The vast majority of students (80.0%) fall between the ages of 17 and 19, which is a typical demographic for first-year college students.

Gender. The gender distribution of the respondents shown in Table 2.

Table 2: Frequency and Percentage Distribution of Respondents by Gender

Gender	Frequency (f)	Percentage (%)
Male	60	60.0%
Female	40	40.0%
Total	**100**	**100.0%**

The data in Table 2 indicates that the respondent pool was predominantly male, comprising **60.0%** of the sample, while female students made up the remaining **40.0%**.

Daily Internet Use. Respondents were asked to report the average number of hours they spend on the internet daily. The results are summarized in Table 3.

Table 3: Frequency and Percentage Distribution by Daily Internet Use

Hours per Day	Frequency (f)	Percentage (%)
Less than 2 hours	13	13.0%
2 to 4 hours	33	33.0%
5 to 7 hours	27	27.0%
8 to 10 hours	15	15.0%

Hours per Day	Frequency (f)	Percentage (%)
More than 10 hours	12	12.0%
Total	**100**	**100.0%**

As detailed in Table 3, the most common duration of internet use was **2 to 4 hours** per day, reported by **33.0%** of the students. A significant majority (**75.0%**) reported using the internet for more than 2 hours but less than 10 hours daily.

2. Level of Cybersecurity Awareness

The second research question assessed the respondents' level of cybersecurity awareness using the Knowledge, Attitude, and Practice (KAP) framework.

a. Knowledge of Cybersecurity

The students' knowledge was assessed with a 10-item test. The overall average score was **5.48 out of 10**, with a standard deviation of 2.15, indicating a **Moderate** level of knowledge. An item analysis, shown in Table 4, revealed significant variance between topics.

Table 4: Summary of Correct Responses for Knowledge Assessment (N=100)

Item No.	Topic	Frequency of Correct Responses (f)	Percentage (%)
7	PII Example	87	87.0%
3	Strongest Password	84	84.0%
1	Purpose of 2FA	75	75.0%
10	New Router Security Step	68	68.0%
6	Public Wi-Fi Protection	64	64.0%
5	Ransomware Definition	48	48.0%
8	Purpose of Updates	40	40.0%
9	Social Engineering Definition	35	35.0%
2	Phishing Example	26	26.0%
4	Meaning of "S" in	17	17.0%

Item No.	Topic	Frequency of Correct Responses (f)	Percentage (%)
	HTTPS		
Average Score		**5.48**	**54.8%**

The findings reveal a sharp divide in the students' knowledge. There is a strong understanding of foundational, static concepts such as identifying Personally Identifiable Information (87%) and creating strong passwords (84%). However, there are critical weaknesses in practical, threat-recognition areas. Knowledge of dynamic threats was extremely low, with only 35% able to define social engineering and only 26% correctly identifying a phishing attempt. The most alarming gap was in web security, where only 17% of students could identify what the "S" in HTTPS stands for, indicating they do not possess the knowledge to identify unsafe websites or common manipulative attacks.

b. Attitude Towards Cybersecurity

Respondents' attitudes were measured using a 10-item Likert scale survey. The overall weighted mean for attitude was **3.69**, which corresponds to a **Positive Attitude**. Table 5 shows the breakdown per item.

Table 5: Weighted Mean of Attitude Towards Cybersecurity

Attitude Statement	Weighted Mean	Interpretation
Q1: Keeping my information secure is important.	4.35	Positive
Q3: Complex passwords are worth the effort.	4.19	Positive
Q7: I am confident in my ability to spot a phishing email.	3.92	Positive
Q5: I believe I am responsible for my own online security.	3.86	Positive
Q4: Regular software updates are essential for	3.81	Positive

Attitude Statement	Weighted Mean	Interpretation
security.		
Q2: Using 2FA is a necessary security measure.	3.75	Positive
Q9: Cybersecurity is an interesting subject for me.	3.63	Positive
Q10: I am willing to pay for security software.	3.48	Neutral
Q6: Public Wi-Fi is generally safe without a VPN. (Reversed)	3.22	Neutral
Q8: It's too much trouble for different passwords. (Reversed)	3.14	Neutral
Overall Weighted Mean	**3.69**	**Positive**
Scale: 4.50-5.00 (Very Positive); 3.50-4.49 (Positive); 2.50-3.49 (Neutral); 1.50-2.49 (Negative); 1.00-1.49 (Very Negative)		

Students generally hold a positive view of cybersecurity. However, a concerning finding is the high score for confidence in spotting phishing emails (3.92-"Positive"). When contrasted with the knowledge test where only 26% could actually do so, this suggests a dangerous level of overconfidence.

c. Cybersecurity Practices

Self-reported cybersecurity practices were measured with a 10-item Likert scale. The overall weighted mean was **3.88**, indicating that students **Often Practice** secure behaviors.

Table 6: Weighted Mean of Cybersecurity Practices

Practice Statement (I use/do...)	Weighted Mean	Interpretation
Q2: I avoid sharing my passwords with anyone.	4.56	Always
Q1: I use strong, unique passwords for important accounts.	4.28	Often
Q4: I lock my computer or phone when I step away.	4.25	Often

Practice Statement (I use/do...)	Weighted Mean	Interpretation
Q5: I think before clicking on links in emails/messages.	4.11	Often
Q3: I use Two-Factor Authentication (2FA) when available.	3.98	Often
Q9: I back up my important files regularly.	3.69	Often
Q10: I review privacy settings on my social media.	3.65	Often
Q8: I keep my software and apps updated.	3.55	Often
Q7: I use a VPN when on public Wi-Fi.	3.42	Sometimes
Q6: I verify the "HTTPS" in the address bar for secure sites.	3.31	Sometimes
Overall Weighted Mean	**3.88**	**Often**
Scale: 4.50-5.00 (Always); 3.50-4.49 (Often); 2.50-3.49 (Sometimes); 1.50-2.49 (Rarely); 1.00-1.49 (Never)		

Students report strong practices in basic password hygiene. However, there is a clear "Knowledge-Attitude-Practice (KAP) Gap." The two lowest-rated practices—using a VPN on public Wi-Fi and verifying HTTPS—are performed only "Sometimes" and directly correspond to the critical knowledge gaps identified earlier. This indicates that a lack of specific knowledge prevents students from performing crucial security actions, despite their positive attitude.

3. Relationship Between Demographic Profile and Cybersecurity Awareness

To test the null hypothesis that there is no significant relationship between the demographic profile (Age, Gender, Internet Use) and the level of cybersecurity awareness (Knowledge, Attitude, Practice), a Pearson correlation analysis was conducted. The significance level (alpha) was set at 0.05. A p-value less than 0.05

indicates a statistically significant relationship. The results are presented in Table 7.

Table 7: Correlation Between Demographic Profile and Cybersecurity Awareness

Demographic Variable	Correlation Results with Cybersecurity Awareness Components
	Knowledge Score
Age	r = -.007 | p = .953
Gender *(0=Male, 1=Female)*	r = .081 | p = .422
Internet Use	r = .180 | p = .073

**Correlation is significant at the 0.05 level.*

The correlation analysis revealed one statistically significant relationship among the nine pairs of variables tested.

- **Significant Finding (Age and Attitude):** The analysis found a **statistically significant, weak positive correlation between Age and Attitude** (r = .211, p = .035). Because the p-value is less than 0.05, this finding is considered significant. It indicates that as age increases within this group of students, there is a discernible tendency for their self-reported attitudes towards cybersecurity to become more positive.
- **Marginal Finding (Internet Use and Knowledge):** The relationship between Internet Use and Knowledge approached significance (r = .180, p = .073). While not statistically significant by the $p < .05$ standard, this "statistical trend" suggests that students who spend more time online may have slightly higher cybersecurity knowledge.
- **Non-Significant Findings:** All other correlations were not statistically significant. Age showed no significant relationship with Knowledge (p=.953) or Practice (p=.166). Gender showed no significant relationship with any of the KAP

components. Similarly, Internet Use was not significantly correlated with Attitude (p=.703) or Practice (p=.140).

Decision on the Hypothesis

The null hypothesis states: *"There is no significant relationship between the demographic profile (Age, Gender, Internet Use) and the level of cybersecurity awareness (Knowledge, Attitude, Practice)."*

- Based on the significant correlation found between Age and Attitude (p=.035), the null hypothesis is **rejected** for this specific relationship.
- For all other relationships tested, the p-values were greater than 0.05, therefore the null hypothesis **fails to be rejected** for those pairs.

The study thus concludes with a **partial rejection of the null hypothesis**. A statistically significant relationship exists between a student's age and their cybersecurity attitude, but not between other demographic variables and the components of cybersecurity awareness.

Chapter V

SUMMARY, CONCLUSION, AND RECOMMENDATION

This chapter presents a concise overview of the study's findings, draws overarching conclusions based on the analysis, and provides actionable recommendations. The content is derived directly from the results detailed in Chapter IV regarding the cybersecurity awareness of first-year IT students at HGBaquiran College.

Summary

The key findings of this research are summarized as follows:

1. **Demographic Profile:** The typical respondent in this study was an 18-year-old male student who spends between 2 to 7 hours on the internet daily. The demographic makeup was consistent with that of a standard first-year college IT program.
2. **Cybersecurity Knowledge:** Students possess a **Moderate** level of cybersecurity knowledge, with an average score of 54.8%. While they demonstrated a good understanding of static concepts like strong passwords, they showed severe deficiencies in identifying active threats. Knowledge was particularly weak in recognizing phishing (26% correct), defining social engineering (35% correct), and understanding web security indicators like HTTPS (17% correct).
3. **Cybersecurity Attitude:** Students hold a generally **Positive** attitude towards cybersecurity (overall mean of 3.69), agreeing that it is important. A significant point of concern was a high level of overconfidence, with students expressing a strong belief in their ability to spot phishing attempts, a belief that was not supported by their actual knowledge scores.

4. **Cybersecurity Practice:** Students reported that they **Often** perform basic security behaviors like password management (overall mean of 3.88). However, a distinct gap was evident, as practices requiring specific technical knowledge—such as using a VPN on public Wi-Fi or verifying HTTPS on websites—were only performed "Sometimes." This directly mirrored their knowledge deficits.
5. **Correlational Analysis:** The study's primary relational finding was a **statistically significant, weak positive correlation between Age and Attitude towards cybersecurity** ($r = .211$, $p = .035$). Furthermore, a "statistical trend" was noted between higher internet use and slightly higher knowledge scores ($p = .073$). No other demographic variables showed a significant relationship with knowledge, attitude, or practice.

Conclusions

Based on the summary of findings, the following conclusions are drawn:

1. **Maturity Influences Cybersecurity Mindset, But Not Application.** The significant positive correlation between age and attitude suggests that even small increases in age and life experience within this young adult cohort contribute to a more serious and positive mindset towards personal security. However, this improved attitude does not independently lead to better knowledge or security practices, confirming that a good mindset alone is insufficient for protection.
2. **A Significant "Knowledge-Attitude-Practice (KAP) Gap" Exists.** This study confirms a critical disconnect. Students *believe* security is important (Positive Attitude) but lack the specific technical understanding (Moderate/Low Knowledge) required to perform crucial security actions consistently (Inconsistent Practice). Their weakest knowledge

areas directly correspond to their least-performed security habits, proving that knowledge is a direct prerequisite for effective practice.

3. **Cybersecurity Deficiency is a Universal, Not Demographic, Issue.** With the exception of attitude being linked to age, the core deficiencies in technical knowledge and security practices are pervasive across the entire student group. The problems are not confined to a specific gender or level of internet use. This indicates that first-year IT students, despite being "digital natives," arrive on campus with a shared set of vulnerabilities, making this an institutional challenge rather than an issue with a subgroup.

Recommendations

Based on the conclusions, the following recommendations are proposed:

For the College Administration and IT Department:

1. **Implement Mandatory, Practical First-Year Security Training.** The universal knowledge gaps necessitate a mandatory, hands-on cybersecurity module integrated into the first-semester IT curriculum. This training must move beyond theory and focus on closing the identified weaknesses through phishing simulations, social engineering case studies, and practical labs on network security (e.g., configuring VPNs, identifying HTTPS certificates).
2. **Leverage Positive Peer Influence.** Given that slightly older students demonstrate more positive attitudes, instructors should be encouraged to identify these students and strategically position them as informal peer leaders in group projects and class discussions related to security. This can help shape a positive security culture and influence the mindset of their younger classmates.

For the Instructors:

1. **Explicitly Bridge the Attitude-to-Action Gap.** Instructors should directly challenge the students' passive positive attitude. This can be done by stating: "It is not enough to believe security is important. It must be practiced." They should then provide direct, non-negotiable actions, such as requiring the use of password managers for class projects or having students enable Two-Factor Authentication on their school accounts as a graded assignment.
2. **Use Local Data to Address Overconfidence.** Instructors can use the data from this very study to confront student overconfidence. By showing students that their peers were highly confident but scored poorly on the phishing identification test, it can help break down their sense of invulnerability and make them more receptive to learning practical defensive skills.

For Future Researchers:

1. **Investigate the "Why" Behind the Age-Attitude Link.** Future studies should employ qualitative methods, such as one-on-one interviews or focus groups, to explore why older students have better attitudes. Understanding whether this is due to maturity, prior work experience, or other life factors can lead to more targeted and effective educational strategies.
2. **Conduct a Comparative Study.** This research should be replicated at other colleges and across different academic departments (e.g., Business, Arts, Education). This would determine if the findings are specific to IT students at one institution or if they represent a broader trend among the general student population.
3. **Evaluate Interventions Using an Experimental Design.** A robust follow-up study could use this research as a baseline. A

new cohort of students could be divided into an experimental group that receives the proposed training module and a control group that does not. By measuring the KAP of both groups before and after, researchers can quantitatively assess the effectiveness of the intervention.

BIBLIOGRAPHY

References

Al-Ghafis, M. A., Ashari, A., Al-Ahdal, A. O., & Al-Hammadi, M. (2022). *Cybersecurity awareness in higher education institutions: A systematic literature review*. Applied Sciences, 12(17), 8826. https://doi.org/10.3390/app12178826

Al-Mhiqani, M. N., Al-Ahdal, A. O., Zaid, M. A., & Batarfi, R. T. (2022). *A cross-sectional study of cybersecurity awareness among It and engineering students: The case of a public university in a developing country.* Applied Sciences, 12(12), 5909. https://doi.org/10.3390/app12125909

Al-shboul, B., Al-Ghuwairi, A. R., Al-Zoubi, A., & Almalki, D. E. (2023). *Assessing cybersecurity knowledge, attitude, and practices (KAP) among university students in Jordan. Annals of Computer Science and Information Systems, 36, 37–43.* https://doi.org/10.15439/2023F2

Hadlington, L. (2017). *Human factors in cybersecurity; a review of the literature. Research Poster. The British Psychological Society, Cyberpsychology Section Conference, 27.*

Olegario, R. M. (2022). *Cybersecurity awareness and practices among senior high school students. International Journal of Computing and Digital Systems, 12(1), 1–11.*

Pitagan, F. B. (2021). *Digital citizenship in the new normal: The Philippine context. International Journal of Digital Society (IJDS), 2(4), 1361–1366.*

Portela, G.-L., & Tovar, E. (2023). *Undergraduates' cyber risk perception, training needs, and the role of higher education. Education and Information Technologies, 28(11), 14389–14413. https://doi.org/10.1007/s10639-023-11804-w*

Tanael, M. A. P., Torres, M. J. L., & Arenas, A. P. (2021). *Cybersecurity awareness among university students in the Philippines. 2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), 1–6.* https://doi.org/10.1109/HNICEM54116.2021.9732104

Yaokumah, W., Brown, S., & Amponsah, R. (2020). *Factors affecting information security compliance intention in higher education. Journal of Information Technology Education: Research, 19, 639-661.* https://doi.org/10.28945/46393. https://doi.org/10.1007/s10639-023-11804-w

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

APPENDICES

APPENDIX A. LETTER

August 26, 2025

THE INSTRUCTOR
HGBaquiran College, Inc.
Tumauini, Isabela

Subject: Request to Conduct Research and Obtain the official count of First-Year IT Students

Dear Ma'am/Sir,

Greetings of peace!

We, the undersigned students pursuing the degree of BS in Information Technology at HGBaquiran College, are currently working on our undergraduate research paper entitled, **"Assessing Cybersecurity Knowledge, Attitudes, and Practices (KAP) Among First-Year Information Technology Students at HGBaquiran College."** This study is a partial fulfillment of the requirements for our course.

The primary objective of this research is to assess the baseline cybersecurity awareness of the first-year IT students. The findings are expected to provide the IT department with valuable data that can aid in curriculum enhancement and the development of targeted training programs, ultimately fostering a stronger culture of security among our future IT professionals.

In this regard, we would like to humbly request permission from your good office for the following:

1. To conduct our study by administering a survey questionnaire to all first-year Information Technology students for the Academic Year 2025-2026.
2. To obtain the official enrolled population of first-year IT students. This will be essential for our census-based approach, which aims to invite every member of the population to participate, thereby ensuring the highest possible accuracy for our findings.

We would like to assure you that all data gathered will be treated with the utmost **confidentiality** and will be used solely for academic purposes, in strict compliance with the Data Privacy Act of 2012 *(RA 10173)*. Furthermore, student participation will be completely **voluntary**, and the survey will be administered at a time convenient for the students to ensure minimal disruption to their classes.

Attached to this letter is a copy of our survey questionnaire for your perusal.

We are hopeful for your positive response to this request. Your support will be instrumental in the successful completion of our study and will contribute significantly to the academic community of our college.

Thank you very much.

Respectfully yours,

Aquino, Clarissa U.

Bacani, Kristel Ann M.

Baccay, Jay Christian

Cayaba, Instien L.

Diaz, Jesus D.
Researchers

Noted by:

Rally T. Melegrito
Research Adviser

APPENDIX B. SURVEY QUESTIONNAIRE

Part I: Demographic Profile

Instructions: *Please provide the following information by writing on the blank or checking (✓) the box that corresponds to your answer.*

1. **Age:** _____
2. **Gender:**
   ☐ Male
   ☐ Female
3. **On an average school day, how many hours do you spend using the internet for both academic and personal reasons?**
   ☐ Less than 2 hours
   ☐ 2 - 4 hours
   ☐ 5 - 7 hours
   ☐ 8 - 10 hours
   ☐ More than 10 hours
   ☐

Part II: Knowledge of Cybersecurity

Instructions: *Please encircle the letter of the best answer for each question. There is only one correct answer for each item.*

1. What is the primary purpose of Two-Factor Authentication (2FA)?

   a. To make your password easier to remember.
   b. To add a second layer of security beyond just a password.
   c. To speed up the login process.
   d. To block advertisements on websites.

2. You receive an unexpected email with a subject line "Urgent: Your Account is Suspended!" asking you to click a link and enter your password to fix it. This is a classic example of:

   a. A virus
   b. Spyware
   c. A phishing attack
   d. A system update

3. Which of the following represents the strongest password?

   a. password123
   b. MyDogSparky
   c. J#p8!z@qY*5v
   d. 12345678

4. What does the "S" in "HTTPS://" signify when you visit a website?

   a. Standard
   b. Site
   c. Social
   d. Secure

5. Which type of malware is specifically designed to lock your files and demand payment for their release?

   a. Ransomware
   b. Adware
   c. Spyware
   d. Trojan horse

6. When using a public Wi-Fi network *(like in a coffee shop or restaurants)*, what is the most recommended practice to protect your data from being intercepted?

   a. Using incognito mode in your browser.
   b. Using a Virtual Private Network (VPN).
   c. Connecting only to websites you trust.
   d. Turning your firewall on the highest setting.

7. Which of the following is considered Personally Identifiable Information (PII) that you should be careful about sharing online?

   a. Your favorite color
   b. Your full name, birthdate, and home address
   c. Your opinion on a movie
   d. Your username in a video game

8. What is the main reason to regularly update the software on your devices *(e.g., operating system, apps)*

   a. To get new visual features and emojis.
   b. To clear up storage space on your device.
   c. To patch security vulnerabilities that have been discovered.
   d. To make the software run faster.

9. "Social engineering" in a cybersecurity context refers to:

   a. Designing better social media platforms.
   b. Manipulating people into divulging confidential information.
   c. The study of how engineers interact in the workplace.
   d. A type of computer programming language.

10. You buy a new Wi-Fi router for your home. What is the most important first security step you should take?

    a. Position it in the center of your house for the best signal.
    b. Change the default administrator password and network name (SSID).
    c. Connect all your devices to it immediately.
    d. Download the router's mobile app.

Part III: Attitudes Towards Cybersecurity

Instructions: *Please indicate your level of agreement with the following statements. Check (✓) the box that best reflects your opinion.*

(5 - Strongly Agree**, 4 -** Agree**, 3 -** Neutral**, 2 -** Disagree**, 1 -** Strongly Disagree**)**

Statement	**5**	**4**	**3**	**2**	**1**
1. I believe that my personal online security is primarily my own responsibility.					
2. Taking a few extra seconds for security measures is worth the effort.					
3. It is extremely important to use a different password for each of my important online accounts *(email, banking, etc.).*					

4. I feel that cybersecurity is a topic that all IT students must take seriously from the beginning of their studies.					
5. I am confident in my ability to recognize a phishing email or a suspicious wbsite.					
6. The risk of being a victim of a cyberattack is low for a student like me.					
7. Regularly backing up my important digital files is a critical habit.					
8. Public Wi-Fi networks are generally safe for logging into personal accounts as long as the website is secure (HTTPS).					
9. Installing software from unknown or untrusted websites is a major security risk.					
10. Sharing personal details on social media can significantly increase my vulnerability to online threats.					

Part IV: Cybersecurity Practices

Instructions: *Please indicate how often you perform the following actions. Check (✓) the box that best describes your actual habits.*

(5 - Always**, 4 -** Often**, 3 -** Sometimes**, 2 -** Rarely**, 1 -** Never**)**

Statement	**5**	**4**	**3**	**2**	**1**
1. I use a combination of letters (upper/lower case), numbers, and symbols in my passwords.					
2. I use a different password for my critical accounts *(e.g., email, social media, banking)*.					
3. Before I click on links in unexpected emails, I check the destination URL first.					
4. I install software updates for my computer's operating system and applications as soon as they are available.					
5. I back up my important files *(e.g., school projects, photos*) to a separate location like a cloud service or external drive.					
6. I review and adjust the privacy settings on my social media accounts.					
7. I lock my computer or smartphone when I step away from it, even for a short time.					
8. I use a VPN when I connect to a public Wi-Fi network to conduct sensitive transactions.					
9. I avoid downloading and installing software from unfamiliar websites or pop-up ads.					
10. I read the permissions an application asks for before I install it on my phone.					

APPENDIX C. RAW SCORES

Respondent	Age	G_C	I_U_C	K_S	A_S (WM)	P_S(WM)
1	18	0	3	6	3.5	3.7
2	18	0	3	5	3.3	2.8
3	19	0	1	5	4.5	4.5
4	18	0	2	8	3.5	3.3
5	19	0	1	7	3	3.2
6	27	0	1	6	4.2	4.1
7	17	0	3	7	4.3	3.1
8	19	0	3	7	2.8	2.6
9	20	0	1	4	3.7	4.4
10	19	0	3	3	3.1	3.9
11	18	0	3	8	3.5	4.2
12	18	0	2	5	5	4.1
13	19	1	2	6	4.3	4.1
14	18	1	3	5	3.4	3.9
15	17	1	4	4	3.5	4
16	18	1	4	3	3	3.5
17	18	1	4	6	2.8	2.8
18	18	1	5	8	4.5	4.6
19	17	1	5	9	3.8	3.6
20	19	1	3	4	4.1	4.3
21	18	1	3	6	2.8	3.9
22	18	1	4	5	4.6	4.6
23	18	1	3	6	2.7	3
24	18	1	5	8	4	4.6
25	18	1	5	10	3.6	4.8
26	17	1	4	5	3.5	3.6
27	18	1	3	6	3.6	4.2
28	17	1	5	5	4.2	3.8
29	17	1	4	6	4.4	3.4
30	19	1	5	10	4.1	4.6
31	17	0	4	4	4	3.5
32	18	0	4	8	3.3	5
33	18	0	2	6	2.5	2.7
34	18	0	4	5	3.2	4.6
35	18	0	5	3	4	4.2
36	18	0	2	6	3.5	2.7
37	18	0	2	5	4.5	4.5
38	27	0	3	1	3.5	3.4
39	18	0	2	8	3.7	3.7
40	18	0	5	4	3.8	4.2

Bacani
Cayaba
Aquino
Diaz

Instructions:

G_C — Gender_Coded : Male =0, Female = 1

I_U_C — Internet_Used_Coded:
1 = Less than 2 hours
2 = 2 to 4 hours
3 = 5 to 7 hours
4 = 8 to 10 hours
5 = More than 10 hours

KNOWLEDGE SCORE (K_S)

Demographic	r value	p value
AGE	-0.007	0.953
GENDER	0.081	0.422
INTERNET USE	0.180	0.073

ATTITUDE (A_S(WM))

Demographic	r value	p value
AGE	0.211	0.035
GENDER	0.081	0.422
INTERNET USE	0.039	0.703

PRACTICE (P_S(WM))

Demographic	r value	p value
AGE	0.140	0.166
GENDER	-0.020	0.851
INTERNET USE	0.149	0.140

Correct Answer
1. B
2. C
3. C
4. D
5. A
6. B
7. B
8. C
9. B
10. B

41	19	0	5	4	3.9	3.7
42	18	0	1	5	3.6	3.7
43	19	0	3	7	4.1	4.7
44	18	0	3	4	4.7	4.8
45	18	0	3	6	4.5	4.8
46	19	0	3	6	3.7	4.7
47	18	0	1	7	3.4	4.8
48	18	0	1	5	2.8	4
49	21	0	4	3	4.2	4
50	18	1	3	6	3.9	3.6
51	18	1	2	4	3.5	3.5
52	18	1	2	6	3.7	4.7
53	18	1	2	6	3.4	3.5
54	18	1	3	6	4.3	4.6
55	17	1	2	6	3.5	3.3
56	18	1	4	5	2.9	4.8
57	17	1	3	2	3.3	2
58	19	1	3	3	2.4	3.1
59	17	1	2	5	2	2.6
60	19	1	2	7	3.1	3.1
61	19	0	3	8	4.5	5
62	19	0	3	5	3.6	4.2
63	20	0	4	7	4.6	4.9
64	18	0	2	3	3.8	3
65	18	0	3	6	4.4	4.9
66	18	0	2	5	4.3	2.3
67	18	0	2	5	3.3	3.1
68	18	0	2	3	5	4.6
69	20	0	2	1	5	2.6
70	17	0	2	4	3.4	3.8
71	18	0	2	6	3.9	4.1
72	24	0	5	9	4.4	5
73	19	0	3	6	4.8	4.6
74	21	0	2	7	3.7	3.5
75	17	0	2	3	4.7	4.6
76	18	0	2	5	3.3	2.9
77	18	0	1	5	3	4.6
78	18	0	1	6	4.4	4.1
79	19	0	1	6	2.9	4.6
80	24	0	2	6	4	4.1
81	19	0	1	6	4	4.7
82	18	0	2	4	4	3

Instructions:

G_C

I_U_C

Gender_Coded : Male =0, Female = 1

Internet_Used_Coded:

1 = Less than 2 hours

2 = 2 to 4 hours

3 = 5 to 7 hours

4 = 8 to 10 hours

5 = More than 10 hours

KNOWLEDGE SCORE (K_S)

Demographic	r value	p value
AGE	-0.007	0.953
GENDER	0.081	0.422
INTERNET USE	0.180	0.073

ATTITUDE (A_S(WM)

Demographic	r value	p value
AGE	0.211	0.035
GENDER	0.081	0.422
INTERNET USE	0.039	0.703

PRACTICE (P_S(WM)

Demographic	r value	p value
AGE	0.140	0.166
GENDER	-0.020	0.851
INTERNET USE	0.149	0.140

Correct Answer
1. B
2. C
3. C
4. D
5. A
6. B
7. B
8. C
9. B
10. B

Instructions:

G_C

Gender_Coded :

83	19	0	2	5	3.8	4.1
84	18	0	2	5	4.3	2.3
85	21	0	3	5	2.5	3.9
86	18	0	2	4	3.4	3.4
87	35	1	1	5	5	4
88	18	1	3	5	4.3	3.8
89	18	1	3	5	4.1	3.9
90	18	1	3	4	3.8	3.9
91	24	1	5	9	4.1	5
92	19	1	3	5	4.3	4.7
93	18	1	2	7	4.3	4.9
94	17	1	3	2	1.3	1.4
95	18	1	3	7	4.1	4.7
96	19	1	1	6	4.6	4.5
97	18	1	1	5	4.5	4.3
98	19	1	2	6	3.9	4.4
99	21	1	3	2	3.7	3.9
100	18	1	1	5	3	3.8

I_U_C

Male =0, Female = 1

Internet_Used_Coded:

1 = Less than 2 hours

2 = 2 to 4 hours

3 = 5 to 7 hours

4 = 8 to 10 hours

5 = More than 10 hours

KNOWLEDGE SCORE (K_S)

Demographic	r value	p value
AGE	-0.007	0.953
GENDER	0.081	0.422
INTERNET USE	0.180	0.073

ATTITUDE (A_S(WM)

Demographic	r value	p value
AGE	0.211	0.035
GENDER	0.081	0.422
INTERNET USE	0.039	0.703

PRACTICE (P_S(WM)

Demographic	r value	p value
AGE	0.140	0.166
GENDER	-0.020	0.851
INTERNET USE	0.149	0.140

Correct Answer
1. B
2. C
3. C
4. D
5. A
6. B
7. B
8. C
9. B
10. B

APPENDIX D. ENGLISH CRITIQUE

CERTIFICATION

This is to certify that the research paper entitled: **"Assessing Cybersecurity Knowledge, Attitudes, and Practices (KAP) Among First-Year Information Technology Students at HGBaquiran College"** written by Clarissa U. Aquino, Kristel Ann M. Bacani, Jay Christian Baccay, Instien L. Cayaba, and Jesus D. Diaz has undergone statistical treatment, analysis, and validation.

This certification is issued to the aformentioned authors for statistical review requirements. Issued this 5th day of December 2025.

RICACYN M. BALABBO, LPT
Statistician

APPENDIX E. STATISTICIAN

CURRICULUM VITAE

CLARISSA U. AQUINO

0951-173-3741

aquinoclarisa144@gmail.com

Brgy. Banig Dy-Abra Tumauini, Isabela

I. PERSONAL INFORMATION

DATE OF BIRTH: December 17th, 2002

PLACE OF BIRTH: Dy-Abra Tumauini, Isabela

AGE: 23

SEX: Female

CIVIL STATUS: Single

CITIZENSHIP: Filipino

RELIGION: Roman Catholic

II. EDUCATIONAL BACKGROUND

TERTIARY:

HGBaquiran College, Inc.

BS in INFORMATION TECHNOLOGY

2022 – 2026

Tumauini, Isabela

SECONDDARY (SENIOR HIGH SCHOOL):

Cumabao Integrated School

TECHNICAL-VOCATIONAL-LIVELIHOOD (TVL)

2020 – 2022

Tumauini, Isabela

SECONDARY (JUNIOR HIGH SCHOOL):

Cumabao Integrated School

2016 – 2020

KRISTEL ANN M. BACANI

0955-768-4750

kristelannbacani4@gmail.com

Brgy. Malamag West Tumauini, Isabela

I. PERSONAL INFORMATION

DATE OF BIRTH: November 21st, 2003

PLACE OF BIRTH: Tumauini, Isabela

AGE: 21

SEX: Female

CIVIL STATUS: Single

CITIZENSHIP: Filipino

RELIGION: Roman Catholic

II. EDUCATIONAL BACKGROUND

TERTIARY:

HGBaquiran College, Inc.

BS in INFORMATION TECHNOLOGY

2022 – 2026

Tumauini, Isabela

SECONDDARY (SENIOR HIGH SCHOOL):

Lanna National High School

GENERAL ACADEMIC STRAND (GAS)

2020 – 2022

Tumauini, Isabela

SECONDARY (JUNIOR HIGH SCHOOL):

Lanna National High School

2016 – 2020

JAY CHRISTIAN BACCAY

0997-643-2312

baccaytom88@gmail.com

Brgy. Lingaling Tumauini, Isabela

I. PERSONAL INFORMATION

DATE OF BIRTH: December 21st, 1999

PLACE OF BIRTH: Marikina City

AGE: 27

SEX: Male

CIVIL STATUS: Single

CITIZENSHIP: Filipino

RELIGION: Roman Catholic

II. EDUCATIONAL BACKGROUND

TERTIARY:

HGBaquiran College, Inc.

BS in INFORMATION TECHNOLOGY

2022 – 2026

Tumauini, Isabela

SECONDDARY (SENIOR HIGH SCHOOL):

Tumauini National High School

SCIENCE, TECHNOLOGY, AND MATHEMATICS (STEM)

2020 – 2022

Tumauini, Isabela

SECONDARY (JUNIOR HIGH SCHOOL):

Tumauini National High School.

2016 – 2020

INSTIEN L. CAYABA

0910-459-3559

cybainstien@gmail.com

Brgy. Pilitan Tumauini, Isabela

I. PERSONAL INFORMATION

DATE OF BIRTH: August 29th, 2003

PLACE OF BIRTH: Tumauini, Isabela

AGE: 22

SEX: Male

CIVIL STATUS: Single

CITIZENSHIP: Filipino

RELIGION: Born Again

II. EDUCATIONAL BACKGROUND

TERTIARY:

HGBaquiran College, Inc.

BS in INFORMATION TECHNOLOGY

2022 – 2026

Tumauini, Isabela

SECONDDARY (SENIOR HIGH SCHOOL):

Tumauini National High School

TECHNICAL-VOCATIONAL-LIVELIHOOD (TVL)

2020 – 2022

Tumauini, Isabela

SECONDARY (JUNIOR HIGH SCHOOL):

Josefina Albano National High School.

2016 – 2020

Delfin Albano

JESUS D. DIAZ

0910-459-3559

jesus.social@proton.me

Brgy. Antagan 2nd Tumauini, Isabela

I. PERSONAL INFORMATION

DATE OF BIRTH: July 24th, 2002

PLACE OF BIRTH: Tumauini, Isabela

AGE: 23

SEX: Male

CIVIL STATUS: Single

CITIZENSHIP: Filipino

RELIGION:

II. EDUCATIONAL BACKGROUND

TERTIARY:

HGBaquiran College, Inc.

BS in INFORMATION TECHNOLOGY

2022 – 2026

Tumauini, Isabela

SECONDDARY (SENIOR HIGH SCHOOL):

Advance Montessori Education Center of Isabela, Inc.

SCIENCE, TECHNOLOGY, AND MATHEMATICS (STEM)

2020 – 2022

Tumauini, Isabela

SECONDARY (JUNIOR HIGH SCHOOL):

Advance Montessori Education Center of Isabela, Inc.

2016 – 2020